# CVE Detail – CVE-2017-1000121

The UNIX IPC layer in WebKit, including WebKitGTK+ prior to 2.16.3, does not properly validate message size metadata, allowing a compromised secondary process to trigger an integer overflow and subsequent buffer overflow in the UI process. This vulnerability does not affect Apple products.

## Threat-Mapped Scoring

Score: 1.5

Priority: P4 - Informational (Low)

## EPSS

EPSS Score: N/A

Percentile: 0.69798

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-190: Integer Overflow or Wraparound

## CAPEC(s)

* CAPEC-92: Forced Integer Overflow

## Affected Products

* cpe:2.3:a:webkitgtk:webkitgtk\+:\*:\*:\*:\*:\*:\*:\*:\*